游戏安全实验室 游戏漏洞 外挂分析

By Discuz! Team and Comsenz UI Team

Archived: 2026-04-05 22:36:51 UTC

概况

以《传奇》为代表的各大游戏私服非法运营活动长期泛滥，在国内游戏地下黑产圈内堪称独树一帜，围绕游戏暴利的争夺导致各大私服运营者之间斗争加剧，频繁利用网络劫持、DDOS等技术手段进行”攻城掠地”，所以私服客户端一直都是顽固病毒家族繁殖传播的沉疴宿疾。为了对抗竞争者、外挂和安全厂商，私服客户端经常捆绑各类Rootkit/Bootkit类顽固病毒，并且盗用冒用正常软件数字签名逃避查杀防御，采用VMP等虚拟机强壳保护对抗分析。作为刚性强需求，普通游戏用户会往往无视安全软件查杀拦截提示，反而主动放行恶意驱动模块的加载，最终导致网络浏览异常、系统蓝屏崩溃、感染盗号木马等严重安全后果。

近期，毒霸安全团队通过“捕风”系统再次监测到一类劫持Rootkit病毒家族的活跃迹象，该病毒家族主要通过各类私服客户端进行捆绑传播，主要通过TDI过滤、DNS劫持、HTTP(s)注入、HOSTS重定向等技术手法篡改用户系统网络数据包，将正常网页访问劫持引流至指定私服网站，并利用安全软件云查杀数据包屏蔽、关机回调重写等手段实现对抗查杀，此外，该家族还针对私服运营竞争对手常用的病毒驱动签名进行屏蔽对抗，实现长期稳定劫持控制用户的目的。

根据其模块pdb路径中的项目名称”fk_undead”，我们将其命名为” 亡灵 ” 家族。 从我们的长期监控数据看，该家族近两年非常活跃，从2017年初开始盗用正规厂商数字签名频繁变种传播，本次变种版本最早出现于2018年10左右，目前该家族呈现活跃趋势，全网累计感染量预估超过50万。

技术分析

该病毒的主要运行流程如下：

病毒驱动从恶意传奇私服客户端层层释放而来，根据系统版本的不同，最终释放不同的驱动文件，我们以其中一个样本为例。

用户打开传奇私服客户端之后，程序释放ntprint.exe到TEMP目录下，ntprint.exe主要负责上报相关配置信息到指定服务器，上报完成后会下载http://183.2.193.147:11153/msvcdlx*.dat到本地，而这个msvcdlx*.dat又会下载4个驱动文件到本地，这4个驱动文件的大致用途如下：

（1）mstxdlx*.dat

以64位系统下释放的驱动（mstxdlx64.dat）为例，它主要的作用是通过劫持用户电脑的网络以及篡改相关系统配置，从而达到拦截杀软云查询以及劫持HTTP的正常访问，具体实现方式如下：

A、注册TDI回调函数，过滤收发包

病毒驱动加载后，对TDI_SEND和TDI_SET_EVENT_HANDLER进行了处理，前者主要是负责网络数据的发包，后者则是负责对接收到网络数据进行处理，对这两个地方进行过滤处理之后，带来的效果就是访问A域名，实际打开的却是B网站。

在TDI_SEND中，通过检测360与其云端的通讯时的关键字段“x-360-ver:”，中断云查询，从而造成云查杀的失效：

在TDI_SET_EVENT_HANDLER中，收到符合规则的请求响应数据后，病毒直接修改数据包，嵌入相应的HTML框架代码进行劫持，劫持后效果如下：

以下则是被篡改插入的数据包代码：

B、 设置IE代理，劫持HTTP访问

通常在设置了TDI过滤之后，就已经实现对网络的全局管理了，而设置IE代理的目的，猜测是为了在病毒驱动被杀软清理后，依旧能够长期劫持网站访问所用。

IE的代理配置信息由云端实时下发，相关配置文件下载地址为106.14.47.210:11054/paclist.dat，可根据需要，实时变换文件内容，文件中的内容为BASE64加密后的信息，解密后为pall.ndypkh.com:50511/auto11037.pac：

链接指向一个混淆后的pac脚本文件，去混淆后内容包含大量私服网站的URL信息，当程序使用IE的代理设置，并且访问到列表中的网站时，就会被统一劫持跳转至114.55.234.27:10000（kusf.com）：

根据对劫持名单的梳理，除去私服网站，被劫持跳转的部分主流网站还有：

C、创建关机回调，劫持DNS和自更新

在关机回调中，该病毒驱动主要做了劫持DNS和自更新这两件事情。

通过访问106.14.47.210:11054/dnlist.dat下载劫持的DNS配置信息，然后在关机回调中设置电脑的DNS，从而完成DNS的修改劫持，虽然目前被修改的DNS是正常的，但由于此配置信息由云端下发，所以不排除后期病毒作者会设置恶意的DNS配置信息：

接着，病毒又会访问120.77.36.184:11054/mstxdlx64_up.dat，下载最新版本的驱动文件，并且随机命名保存，然后以服务的方式在下次开机时自启动，完成更新：

D、 创建映像加载回调，拦截其它病毒运行

在映像加载回调中，为了确保被感染的电脑能够被自己成功劫持，当检测到当前加载的是驱动程序时，还会对比签名是否为黑名单中的签名（黑名单从106.14.47.210:11054/bctlist.dat下载而来），若符合拦截规则，则直接禁止加载，黑名单中的驱动签名如下，这些签名大多曾被同类型病毒盗用过，用来给自身恶意程序签名：

E、 创建注册表回调，保护自身启动

在注册表回调中，若发现有对IE代理设置和驱动服务类注册表项的操作，则直接拒绝访问，防止相关注册表项被修改。

除此之外，病毒还会循环枚举注册表回调函数的地址，若检测到被删除，则会再次注册回调函数，这么做为了防止用户利用pchunter之类的ARK工具对回调函数进行删除操作，使病毒难以被手动清除。但如果是病毒程序自身升级需要修改相关的注册表项时，则会利用开关标记来暂停对相关注册表项的保护。

F、 下载配置信息，实时更新劫持信息

上述的整个劫持的流程，无需与3环进程交互，完全由0环的驱动实现，而相关的配置信息，也统一从远程服务器下载，具体的配置文件信息如下：

（2）msdvdlx*.dat

该驱动加载后，会在下次开机时，劫持svchost进程对本地hosts文件的访问，本地hosts的基本作用是把一些常用的域名和IP关联起来，当用户输入一个网址时，会先从本地的hosts文件寻找对应的IP，从而加速解析的速度，但如果劫持了本地hosts文件的话，就可能返回错误的IP地址。

该病毒驱动主要通过注册一个关机回调函数，在该回调函数中加载释放netmsvc.dll到system32目录下，然后注册NetMSvc这个服务项，以确保之后每次开机都能正常加载这个DLL。而netmsvc.dll又释放驱动cbfltfs3.sys到了TEMP目录下，这个cbfltfs3.sys是Callback Technologies公司提供的一个的文件过滤器驱动：

其封装了大量的文件操作API供使用者使用，在netmsvc.dll中，通过添加对hosts文件的拦截规则，即：当svchost进程访问etc目录下的hosts文件时，则会重定向到ringend.mid：

ringend.mid这份劫持名单，由netmsvc.dll从http://106.14.47.210:11153/hstslist.dat下载而来，伪装成系统声音文件保存在C:\Windows\media\下，其内容则是被劫持的域名和要跳转到IP，部分会被劫持的网站截图如下：

当访问的正常网站被劫持后，访问到的结果如下：

而msdvdlx*.dat自己也会实时从120.77.36.184:11153/msdvdlx32_up.dat下载更新，升级自身：

（3）mshsdlx*.dat

该驱动主要用于安装根证书，从而劫持使用了HTTPS的网站。

驱动加载后，会释放证书文件到c:\Windows\SSL下并安装，释放出来的Sample CA 2.cer是一个根证书，会以受信任的根证书颁发机构形式安装到系统中，这一步主要是为了后续在对HTTPS网站进行劫持时，浏览器不会发出警告，而这也是常见的中间人攻击的方式。

相关的劫持列表信息会从http://106.14.47.210:11153/nflist.dat下载，之后访问未被劫持HTTPS网站时，会发现证书为：

而当你访问被劫持的HTTPS网站时，则会在网页中插入跳转代码，跳转到设置好的私服页面，被劫持的部分规则如下：

（4）msadsdlx*.dat

该驱动会下载运行msadapdlx*.dat，由于下载链接已失效，暂不清楚具体行为，不过根据PDB的名称fk_adswindll*.dll，猜测可能用于广告目的。

IOC

PDB信息：

> D:\Work\git\driver\fk_undead\tempobj\rel_x64\fk_drv64\fk_drv.pdb
>
> D:\Work\git\driver\fk_undead\tempobj\rel_x32\fk_maindrv\fk_maindrv.pdb
>
> D:\Work\git\driver\fk_undead\tempobj\rel_x32\fk_svcsdll\fk_svcsdll.pdb
>
> fk_adswindll32.pdb
>
> fk_netfltdll32.pdb

MD5：

> 4889063c79d1f020a6e66a5bbbc67a7a
>
> d13663cacf144c64d2ec5ec9e17cc4e4
>
> d46df4bc4b5ef88c96be76f22556b3cd
>
> b69c1f02c9b5591ddf6396d220055e16
>
> 98fc3fc117ca3f20366a1cf06b985854
>
> 5a15eb8a362c1d409b9ebe1715bf0999
>
> ec617ac421207c8decb7dc329e2ec4ec
>
> 9a10a008e479ce7cf9f4539ec5345a93
>
> 4bea9b46142e24ea8b15a645773a094a
>
> d8decc0b64f8c34490b43f1a748e2ce5
>
> 73c3dc37a7ff5ea5c2ae8834a504e748
>
> 83505258cd10da2080e33fd995b18e86
>
> 852fc34ab0ffc0596ab4ce2527e5ecfa
>
> 79b3189e2f1e9c7583523aa905f05777
>
> 549b186ead42123725b157346b025159
>
> 40d94961bddb12d06ea324a52e6a3248
>
> 7774822f89a5ae69e4dc4a8eee1b0141
>
> c7304f07edee09f6235c125bb5588c8d
>
> e20e9605e09c4145ead51af16415f2af

> a811f6d783c2cdca2b8dc488369bf05e
>
> fccdf8b186b420fe45bd8d829011d45f
>
> 1489fc0e1c5bca573ac35a1a19930f06

域名信息：

> dlx.qyrgy.com
>
> dlx1.qyrgy.com
>
> 183.2.193.147
>
> 106.14.47.210
>
> 120.77.36.184
>
> 180.76.235.211（酷搜服 kusf.com）
>
> ssyl.jbjfrx.com:31355
>
> 182.61.55.53:82/index2.html

原文来自：Freebuf-安全豹

原文链接：https://www.freebuf.com/articles/system/198869.html
